(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 28 493 A 1**

(51) Int. Cl.[7]:
H 04 L 12/46
H 04 L 12/64
G 06 F 13/14

(21) Aktenzeichen: 101 28 493.4
(22) Anmeldetag: 12. 6. 2001
(43) Offenlegungstag: 3. 1. 2002

DE 101 28 493 A 1

(30) Unionspriorität:
595950 16. 06. 2000 US

(71) Anmelder:
International Business Machines Corp., Armonk, N.Y., US

(74) Vertreter:
Teufel, F., Dipl.-Phys., Pat.-Anw., 70569 Stuttgart

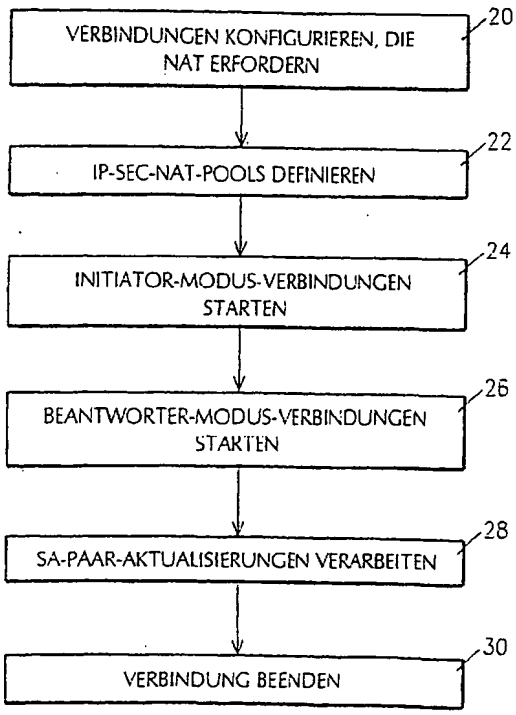
(72) Erfinder:
Boden, Edward B., Vestal, N.Y., US; Monroe, Tod A., Maine, N.Y., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) System und Verfahren zur Integration der Netzwerkadressen-Übersetzung mit IP-Sicherheit

(57) IP-Sicherheit wird in einem virtuellen privaten Netzwerk unter Verwendung von Netzwerkadressen-Übersetzung (NAT) mittels einer oder einer Kombination der vier VPN-NAT-Typen VPN-NAT-Typ-a-Quelle-ausgehend-IP-NAT, VPN-NAT-Typ-b-Ziel-ausgehend, VPN-NAT-Typ-c-eingehend-Quelle-IP-NAT und VPN-NAT-Typ-d-eingehend-Ziel-IP-NAT bereitgestellt. Dies schließt die dynamische Erzeugung von NAT-Regeln und deren Verknüpfung mit den manuell oder dynamisch erzeugten (IKE) Sicherheitszuordnungen vor Beginn der IP-Sicherheit, die die Sicherheitszuordnungen verwendet, ein. Wenn dann IP-Sec bei eingehenden und ausgehenden Datagrammen durchgeführt wird, wird auch die NAT-Funktion durchgeführt.



DE 101 28 493 A 1

Beschreibung

Hintergrund der Erfindung

Querverweise auf damit verbundene Anmeldungen

[0001] Diese Anmeldung ist Continuation-In-Part(CIP) von Seriennummer 09/240 720, eingereicht am 29.01.1999, mit dem Titel "System and Method for Network Address Translation Integration With IP Security".

[0002] US-Patentanmeldung, Seriennummer 09/239 693, eingereicht am 29.01.99, mit dem Titel "System and Method for Managing Security Objects"; Seriennummer 09/240 718, am 29.01.99, mit dem Titel "System and Method for Dynamic Macro Placement of IP Connection Filters"; S/N 09/239 694, eingereicht am 29.01.99, mit dem Titel "System and Method for Dynamic Micro Placement of IP Connection Filters"; S/N 09/240 483, eingereicht am 29.01.99, mit dem Titel "System and Method for Central Management of Connections in a Virtual Private Network, und Seriennummer 09/578,215, eingereicht am 23.05.99, mit dem Titel "System and Method for Network Address Translation Integration with IP Security", werden dem selben Rechtsnachfolger zugewiesen und enthalten in bestimmten Punkten Themen der vorliegenden Anmeldung. Die oben angegebenen Patentanmeldungen sind durch Bezugnahme hier enthalten.

Technischer Bereich der Erfindung

[0003] Diese Erfindung betrifft die Sicherheit von Verbindungen virtueller privater Netzwerke (virtual private network connections) (VPN) und bezieht sich im Besonderen auf VPN-NAT oder die gleichzeitige Verwendung von Netzwerkadressen-Übersetzung (network address translation) (NAT) und Internetprotokoll-(Internet Protocol) (IP) Sicherheits-(IPSec)-Protokolle (Security (IPSec) protocols).

Stand der Technik

[0004] Virtuelle private Netzwerke (virtual private networks) (VPNs) stellen einen aktiven Bereich technischer Entwicklung des gesamten Internets und der Computerindustrie dar. Dies liegt daran, dass sie für die meisten Formen von elektronischem Handel eine grundlegende Voraussetzung darstellen. VPNs verwenden Protocol Tunneling sowie Verschlüsselungs- und Entschlüsselungstechnologie (IP-Sicherheitsprotokolle), um Clients und Servern, Niederlassungen oder unabhängigen Organisationen die Nutzung des Internets für ihren TCP/IP-Verkehr zu wesentlich niedrigeren Kosten zu ermöglichen, als beim Kauf von Standleitungen anfallen, ohne den wichtigsten Vorteil von Standleitungen einzubüßen: Privatsphäre.

[0005] Das Tunneling, das VPN einsetzt, hat eine Nebenwirkung, die ein Problem verursacht: zwei Teilnetze oder Unternehmen oder andere Benutzer, die am Anfang nicht direkt miteinander kommunizierten, tun dies nun, was die Wahrscheinlichkeit von IP-Adressenkonflikten erheblich vergrößert Netzwerkadressen-Übersetzung (Network Address Translation) (NAT) wird im Internet und in Unternehmen, die sich mit dem Internet verbinden, häufig eingesetzt, um Adressenkonflikte zu überwinden. Diese Konflikte ereignen sich gewöhnlich zwischen festgelegten "privaten" Adressräumen (d. h. 10.*.*.*)

[0006] Jedoch stehen NAT und IP-Sicherheit (IP-Sec) architektonisch miteinander in Konflikt. In der Tat wird IP-Sec durch NAT beeinträchtigt. Das heißt, NAT "ist die Funktion, die letztendlich die semantische Überladung der IP-Adresse sowohl als ein Lokalisierer als auch als der Endpunkt-Kennzeichner aufbricht" (siehe "Architectural Implications of NAT", draft-iab-nat-implications-00.txt, März 1998. IPSec wird beschrieben in Kent, S., and Atkinson, "Security Architecture for the Internet Protocol", RFC2401, November 1998; Kent, S., and Atkinson, "IP Authentication Protocol", RFC 2402, November 1998; and Kent, 5., and Atkinson, "IP Encapsulation Security Payload", RFC 2406, November 1998.) Folglich können zwei Hosts keine IP-Sec-Verbindung aufbauen, wenn sich dazwischen ein NAT-System befindet. Dafür gibt es zwei Gründe: für den IP-Verkehr zwischen den beiden Hosts (für die IP-Sec-Verbindung) wird das Berechtigungsprotokoll (AH) oder Verkapselung der Sicherheitsnutzinformation (encapsulation security payload) (ESP) angewandt. (Siehe RFCs 2402 und 2406, oben.)

[0007] Erstens ist bezüglich des Tunnelmodus die IP-Adresse, die übersetzt werden muss, im ESP-Tunnel, und sie ist verschlüsselt. Aus diesem Grund ist sie für NAT nicht verfügbar. Bezüglich des Berechtigungsprotokolls (AH) im Transport- oder Tunnelmodus, ist die IP-Adresse, die übersetzt werden muss, in NAT sichtbar, doch die AH-Berechtigungserkennung (authentication) enthält sie. Daher wird durch Ändern der IP-Adresse die Berechtigungserkennung am fernen Ende der IP-Sec-Verbindung unterbrochen. Bezüglich des ESP im Transportmodus ist die IP-Adresse für NAT verfügbar, selbst wenn ESP mit Berechtigungserkennung verwendet wird. Wenn jedoch die IP-Adresse geändert wird, wird die IP-Sec-Verbindung aufgrund der Unterbrechung der Berechtigungserkennung am fernen Ende der IP-Sec-Verbindung unterbrochen.

[0008] Zweitens, selbst wenn der IP-Verkehr für die IP-Sec-Verbindung übersetzt werden könnte, würde sie fehlschlagen, weil die IP-Sec-Verbindung auf Sicherheitszuordnungen (security associations) basiert, die die beiden Host-IP-Adressen (host IP addresses) enthalten. Diese sind grundlegend für die Sicherheitszuordnungsarchitektur (Security Association architecture) (siehe RFC 2401, oben), insofern die eingehende IP-Sec auf dem Host, auf dem die Entschlüsselung (oder Berechtigungserkennung) zu erfolgen hat, in dreifacher Weise eindeutig bestimmt werden muss:
{Ziel-IP-Adr, SPI, IP-Sec-Protokoll}.
dabei ist SPI der Sicherheitsprotokollindex (security protocol index) (siehe RFC 2401, oben) Angenommen bei gegebenen Hosts A und W wird NAT auf ein IP-Datagramm (ein Gattungsbegriff für Bytes, die in die Leitung geschickt werden) angewandt, wobei sich ESP im Transportmodus befindet, der von A bis W reicht. Folglich wird die IP-Quellenadresse (IP source address) geändert. Wenn das Paket bei W eintrifft, wird es wahrscheinlich erfolgreich entschlüsselt, da dies nicht von der IP-Quellenadresse abhängt (die genau genommen unverschlüsselt, also nicht getunnelt war). Bei ex-

akter Ausführung wird die Prüfung der eingehenden SPD, die auf die Entschlüsselung folgen sollte, wegen der geänderten IP-Quellenadresse fehlschlagen (da es nicht die Adresse war, die bei der Verhandlung über die Sicherheitszuordnung (security association) verwendet wurde). Daher scheitert sogar der Fall des Transportmodus-ESP.

[0009] NAT und IP-Sec einfach gegenseitig auszuschließen, ist keine Lösung, die dem Stand der Technik entspricht. NAT wird sehr häufig eingesetzt, da sie viele Probleme löst, beispielsweise: sie maskiert globale Adressenänderungen, verringert die Adressenbenutzung, verringert die Unterstützungslast von Internetdienstanbietern (ISP) und ermöglicht die gemeinsame Nutzung von Lasten als virtuelle Hosts.

[0010] Dennoch wird NAT als die größte einzelne Bedrohung für die Sicherheitsintegration (security integration) betrachtet, die heutzutage im Internet eingesetzt wird. Dieses "NAT-Problem", wie es nach wie vor bezeichnet wird, ist architektonisch grundlegend. Auch Altanwendungen und -dienste (beispielsweise diejenigen, die für IP Version 4 entwikkelt wurden) werden ihr Nebeneinanderbestehen noch lange fortführen, während Anwendungen und Dienste für IP Version 6 weiterentwickelt werden. Folglich herrscht beim Stand der Technik eine starke Notwendigkeit für die Bereitstellung eines Nebeneinanderbestehens von NAT und IP-Sec, zumindest in ausgewählten Situationen, ohne dass deshalb schwerwiegende Konfigurationsprobleme entstehen. (IP Version 4 wird in "Internet Protocol", RFC791, September 1981, beschrieben. IP Version 6 wird in Deering, S., Hinden, R., "Internet Protocol, Version 6 (IPv6) Specification", RFC2460, Dezember 1998, beschrieben.)

[0011] Eine VPN-Verbindung zwischen zwei Adressendomänen (address domains) kann bewirken, dass zwei Domänen direkt miteinander verbunden werden, obwohl dies höchstwahrscheinlich nicht geplant war. Daher werden durch die vermehrte Verwendung von VPNs die Adressenkonflikte (address conflicts) wahrscheinlich vergrößert. Es wird auch verstanden werden, dass VPNs die Netzwerksichtbarkeit (network visibility) neu definieren und die Wahrscheinlichkeit von Adressenkollision (address collision) beim Durchqueren von NATs vergrößern. Adressverwaltung im Verborgenen hinter NATs wird zu einer beträchtlichen Belastung. Daher besteht beim Stand der Technik die Notwendigkeit, diese Belastung zu verringern.

[0012] In der US-Patentanmeldung, Seriennummer 09/240 720, wird eine Lösung für dieses allgemeine Problem der Integration von IP-Sec und NAT vorgestellt. In einem virtuellen privaten Netzwerk, das Netzwerkadressen-Übersetzung (network address translation) (NAT) verwendet, wird IP-Sicherheit mittels Durchführung einer oder einer Kombination aus vier Typen von VPN-NAT (VPN NAT) bereitgestellt. (Die Beschreibung von drei VPN-NAT-Typen von der Rechtsnachfolger-Akte END9 1999 0129 US1 ist von jetzt an hier enthalten, und der vierte Typ ist Gegenstand dieser Anmeldung.) Dieser umfasst dynamisch erzeugte NAT-Regeln und deren Verknüpfung mit den manuell oder dynamisch erzeugten Sicherheitszuordnungen (security associations) für den Austausch von Internetschlüsseln (Internet key exchange) (IKE) vor Beginn der IP-Sicherheit, die die Sicherheitszuordnungen (security associations) verwendet. (Siehe Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)" RFC2409, November 1998. Der Begriff 'Sicherheitszuordnungen' (Security Associations) ist definiert in RFC201, oben.) Wenn dann IP-Sec bei eingehenden und ausgehenden Datagrammen durchgeführt wird, wird auch die NAT-Funktion durchgeführt. "IP-Sec durchführen" bedeutet, dass die Schritte, die die ausgehende oder eingehende IP-Sec-Verarbeitung umfasst, ausgeführt werden, wie oben durch die drei IP-Sec-RFCs (und andere) definiert. "NAT durchführen" bedeutet, dass die Schritte ausgeführt werden, die die VPN-NAT-Verarbeitung umfassen, wie nachstehend in dieser Anmeldung beschrieben.

[0013] In der US-Patentanmeldung, Seriennummer 09/240 720, muss der Kunde jede einzelne VPN-NAT-Regel als eine getrennte VPN-Verbindung konfigurieren. Dies ist zeitaufwendig und fehleranfällig, und VPN-Verbindungen sind eigentlich dafür gedacht, den Verkehr zu schützen und sollten nicht von speziellen VPN-NAT-Regeln abhängen. Das heißt, die Regeln wurden bis jetzt eins-zu-eins umgesetzt, so dass NAT die Anzahl der erforderlichen VPN-Verbindungen erhöht.

[0014] Es ist eine Aufgabe der Erfindung, ein verbessertes und stark vereinfachtes System und Verfahren für die gleichzeitige Ausführung von Netzwerkadressen-Übersetzung (NAT) und IP-Sicherheit (IP-Sec) bereitzustellen.

[0015] Weiterhin ist es eine Aufgabe der Erfindung, ein System und ein Verfahren zur Herabsetzung der erhöhten Wahrscheinlichkeit von IP-Adressenkonflikten bereitzustellen, die ein virtuelles privates Netzwerk (VPN) mit sich bringt.

[0016] Weiterhin ist es eine Aufgabe der Erfindung, ein System und ein Verfahren für die Nutzung von VPNs bereitzustellen, ohne dass eine Neuadressierung einer Domäne (eine teure Alternative) erforderlich wird.

[0017] Weiterhin ist es eine Aufgabe der Erfindung, ein System und ein Verfahren für VPN-NAT bereitzustellen, das ohne erforderliche Änderungen in Domänenhosts vollständig im IP-Sec-Gateway zustande gebracht werden kann.

[0018] Weiterhin ist es eine Aufgabe der Erfindung, ein System und ein Verfahren für VPN-NAT bereitzustellen, das keine oder nur kleinere Änderungen am Routing in jeder verbundenen Domäne erfordert.

[0019] Weiterhin ist es eine Aufgabe der Erfindung, ein System und ein Verfahren für VPN-NAT bereitzustellen, das einfach zu konfigurieren ist.

[0020] Weiterhin ist es eine Aufgabe der Erfindung, eine Lösung für die Adressenkollisionsprobleme (address collision problems) bereitzustellen, die von VPNs verursacht werden.

[0021] Weiterhin ist es eine Aufgabe der Erfindung, eine vereinfachte Lösung für die Konfiguration von VPN-Verbindungen durch Kunden bereitzustellen.

[0022] Weiterhin ist es eine Aufgabe der Erfindung, einer einzelnen VPN-Verbindung die Unterstützung mehrerer VPN-NAT-Regeln zu ermöglichen.

[0023] Weiterhin ist es eine Aufgabe der Erfindung, ein System und ein Verfahren bereitzustellen, das Konflikte unter den implizit oder dynamisch zugeordneten VPN-NAT-Regeln systemübergreifend vermeidet.

[0024] Weiterhin ist es eine Aufgabe der Erfindung, ein System und ein Verfahren bereitzustellen, das die Systemverwaltungszeit für dynamische NAT-Regeln durch Beseitigung der Notwendigkeit der Verwaltung zahlreicher einzelner VPN-Verbindungen für jede NAT-Regel verringert.

[0025] Weiterhin ist es eine Aufgabe der Erfindung, ein VPN-NAT-System und -Verfahren bereitzustellen, das die Netzwerküberwachung (network monitoring) und die Verkehrsanalyse (traffic analysis) vereinfacht.

Zusammenfassung der Erfindung

[0026] Gemäß der Erfindung wird ein System und ein Verfahren zur Integration von Netzwerkadressen-Übersetzung innerhalb eines gesicherten virtuellen privaten Netzwerks bereitgestellt. Ein interner Netzwerkhost wird dazu konfiguriert, ausgewählten Verkehr an eine Proxy-Netzwerkadresse zu senden. Ein Gateway eines virtuellen privaten Netzwerks wird mit einer Zuordnungstabelle mit Übersetzungsregeln für Netzwerkadressen (network address translation rules) konfiguriert. Als Reaktion auf die Übersetzungsregeln für Netzwerkadressen wird dann eine virtuelle private Netzwerkverbindung gestartet.

[0027] Andere Merkmale und Vorteile dieser Erfindung werden anhand der folgenden ausführlichen Beschreibung der vorliegenden bevorzugten Ausführungsform der Erfindung in Verbindung mit den begleitenden Zeichnungen deutlich.

Kurze Beschreibung der Zeichnungen

[0028] **Fig.** 1 ist ein Flussdiagramm des VPN-NAT-Verfahrens der bevorzugten Ausführungsform der Erfindung.

[0029] **Fig.** 2 veranschaulicht vom Ziel ausgehende NAT, die mit von Quellen ausgehender NAT verwendet wird, um es zwei Teilnetzen mit identischen Teilnetzen zu ermöglichen, gemäß der bevorzugten Ausführungsform der Erfindung zu kommunizieren.

[0030] **Fig.** 3 veranschaulicht statische NAT, die einfachste konventionelle NAT zur Darstellung des Zusammenhangs.

[0031] **Fig.** 4 veranschaulicht Maskeraden-NAT (masquerade NAT), eine Art von konventioneller NAT zur Darstellung des Zusammenhangs.

[0032] **Fig.** 5 ist ein Übersichts-Flussdiagramm, das die Beziehungen zwischen verschiedenen Programm- und Datenelementen veranschaulicht, die das System und das Verfahren der Erfindung einsetzt.

[0033] **Fig.** 6 veranschaulicht VPN-NAT, Typ b (bekannt als "Zielaus") (destination-out), gemäß der bevorzugten Ausführungsform der Erfindung.

[0034] **Fig.** 7 ist ein Diagramm, das die Überschneidung von Adressendomänen und die Bedingungen veranschaulicht, unter denen "Zielaus"- (destination-out) und "Quelle-aus" (source-out)-Netzwerkadressen-Übersetzung erforderlich ist.

Bevorzugte Ausführungsart der Erfindung

[0035] Gemäß der bevorzugten Ausführungsform der Erfindung wird das NAT-Problem durch Funktionen angegangen, die statt einer einzigen NAT-Übersetzungsregel VPN-NAT mit mehreren NAT-Übersetzungsregeln enthält, die für eine einzelne VPN-Verbindung gültig sind. Dies vereinfacht die Konfiguration durch den Kunden erheblich. Zuvor musste jede Adresse, die NAT und VPN erfordert, getrennt konfiguriert werden. Hinsichtlich der Vorangegangen US-Patentanmeldung, Seriennummer 09/240 720, wird für "Typ a Quelle-aus" und "Typ d Ziel-ein"-VPN-NAT in ebenfalls anhängiger Patentanmeldung Seriennummer 09/578,215 sowie in der vorliegenden Anmeldung für "Type b Ziel-aus" zusätzliche Funktion bereitgestellt. Um nichtfunktionierende IP-Sec-Verbindungen mit der versehentlichen Verwendung von VERBERGEN- und ZUORDNEN-NAT-Regeln (bekannt als "konventionelle NAT") zu vermeiden, wird während der konventionellen NAT auf AH oder ESP überprüft. VERBERGEN- und ZUORDNEN-NAT-Regeln sind zwei grundlegende Formen konventioneller NAT, die in Verbindung mit den **Fig.** 3 und 4 nachfolgend beschrieben werden. Wenn eine gegebene NAT-Regel für das IP-Paket (IP packet), außer für den AH- oder ESP-Kopf (header) gültig ist, wird keine Adressenübersetzung (address translation) durchgeführt. Dies gilt für eingehende und ausgehende NAT. Daher wird für konventionelle NAT (im Vergleich zu VPN-NAT für IP-Sec oder IP-Sec-NAT) IP-Sec bevorzugt. IP-Sec hat Vorrang vor konventioneller NAT.

[0036] Da zu dem Zeitpunkt, da die NAT-Regeln geladen werden, nicht bekannt ist, ob irgendwelche IP-Sec-Verbindungen miteinander in Konflikt (z. B. dynamisches IP) stehen könnten, kann die Überprüfung solcher Probleme erst bei der tatsächlichen NAT-Verarbeitung im Betriebssystemkernel erfolgen. Wenn die Journalerstellung für die Regel aktiviert (on) ist, wird Benutzer-Sichtbarkeit (user visibility) für diese Aktionen gewährt, indem in einem Journaleintrag angezeigt wird, dass eine NAT-Regel in das Datagramm passt, jedoch wegen IP-Sec nicht durchgeführt worden ist. Zusätzlich kann eine Protokollierung der Betriebssystemkernel-Informationen dieser Aktionen für eine begrenzte Anzahl von Vorkommen pro konventioneller NAT-Regel bereitgestellt werden. Ähnlich kann auch eine Nachricht pro Verbindung statt pro Vorkommen im Jobprotokoll eines Verbindungsmanagers oder in einem Verbindungsjournal bereitgestellt werden.

[0037] "Journalerstellung" und "Journaleintrag" sind Begriffe, die sich auch auf das beziehen, was gewöhnlich als "Protokollierung" bzw. "Protokolleintrag" bekannt ist.

[0038] Um zu ermöglichen, dass gemäß der in der Stammanmeldung beschriebenen Erfindung, auf die als VPN-NAT Bezug genommen wird, NAT am IP-Sec-Gateway mit IP-Sec verwendet wird, behalten Kunden private interne IP-Adressen bei. Erhöhte Adressenkollision wird dadurch vermieden, dass IP-Sec-Verbindungen am IP-Sec-Gateway beginnen und enden. Ein IP-Sec-Gateway ist ein Begriff, der in RFC2401, oben, definiert ist. Der Begriff "VPN-Verbindung" ist ein weiterer Begriff, der sich auf das bezieht, was gewöhnlich mit "IP-Sec-Tunnel" ("IP-Sec tunnel") bezeichnet wird, wobei letzterer in RFC2401, oben, definiert wird.

[0039] Weiterhin werden gemäß der Stammanmeldung virtuelle private Netzwerke (VPN) sowohl im Initiator- als auch im Beantworter-Modus mit einer integrierten NAT-Funktion bereitgestellt. Sicherheitszuordnungen (security associations) werden unter Verwendung der korrekten externen (NAT-rts) IP-Adressen ausgehandelt, und die Netzwerkadressen-Übersetzung entsprechender interner (NATlks) IP-Adressen erfolgt durch erzeugte NAT-Regeln synchron mit der Verbindungslast für IPsec- und IPSec-Verarbeitung im Betriebssystemkernel. Eingehende Quelle-IP-Adressen werden genau wie die übliche Quelle-IP-Adressen-NAT bei Ausgang (mit entsprechender Übersetzung der Ziel-IP-Adresse bei Eingang) übersetzt. Eine "VPN-NAT-Regel" wird in **Fig.** 3 durch die Blöcke **72** und **76** dargestellt; das heißt, die beiden lks- und rts-Adressensätze umfassen eine VPN-NAT-Regel.

[0040] Gemäß der vorliegenden Erfindung unterstützt eine einzelne VPN-Verbindung mehrere VPN-NAT-Regeln, indem sie dem Kunden die Angabe einer Klasse von NAT-Regeln ermöglicht, die mit einer VPN-Verbindung verknüpft sind, und ermöglicht es dem System, eine spezielle NAT-Bindung (Regel) aus dieser Klasse dynamisch zu erzeugen. Weiterhin werden Konflikte zwischen den implizit oder dynamisch zugeordneten VPN-NAT-Regeln durch Verknüpfung kundenkonfigurierter NAT-Adresspools mit lokalen IP-Adressen systemweit vermieden, wenn der VPN-NAT-Typ quelleneingehend ist. Die vier VPN-NAT-Typen werden in Tabelle 1, unten, definiert.

[0041] In Bezug auf **Fig. 1** umfasst das Verfahren der bevorzugten Ausführungsform der Erfindung für die Ausführung von VPN-NAT in Schritt **20** das Konfigurieren von Verbindungen, die NAT erfordern, in Schritt **22** das Definieren von IPsec-NAT-Adresspools, in Schritt **24** das Starten von Verbindungen im Initiator-Modus, in Schritt **26** das Starten von Beantworter-Modus-Verbindungen (diese werden am anderen Ende der Verbindung gestartet), in Schritt **28** die Verarbeitung von SA-Paar-Aktualisierungen sowie in Schritt **30** die Beendigung der Verbindungen. (Ein NAT-Pool besteht aus einer Anzahl von IP-Adressen.) Jeder dieser Schritte wird unten näher erklärt.

[0042] In Schritt **20** entscheidet der Benutzer über die Verbindungen, die NAT erfordern und konfiguriert diese Verbindungen. Dies ist logisch gleichbedeutend mit dem Schreiben von NAT-Regeln. Die vier Fälle, bei denen dieses Vorgehen in Betracht zu ziehen ist, sind in Tabelle 1 dargestellt.

TABELLE 1

TYPEN VON VPN-NAT

	IDci (Quelle)	IDcr (Ziel)
Initiator-Modus	Quelle-aus Typ a.NAT interne Adresse, IP-Quelle bei Ausgang, IP-Ziel bei Eingang.	Ziel-aus Typ b.NAT
Beantworter-Modus	Quelle-ein Typ c.NAT externe Adresse, IP-Quelle bei Eingang, IP-Ziel bei Ausgang,	Ziel-ein Typ 4.NAT interne Adresse, IP-Ziel bei Eingang, IP-Quelle bei Ausgang.

wobei
IDci = "Kennzeichner des Client-Initiators"
IDcr = "Kennzeichner des Client-Beantworters".

[0043] Eine VPN-Verbindung besitzt definitionsgemäß vier Endpunkte:
zwei "Verbindungsendpunkte" und zwei "Datenendpunkte". (Transportmodus bedeutet dann, dass der Verbindungsendpunkt gleich dem Datenendpunkt an jedem Ende der Verbindung ist.) Die Begriffe IDci und IDcr beziehen sich insbesondere auf die beiden Datenendpunkte, indem sie anzeigen, welcher der Initiator und welcher der Beantworter ist (siehe RFC2409, oben.) Diese Kennzeichner können eine von ungefähr sechs verschiedenen Formen annehmen, die Teil der IDci, IDcr-Definitionen sind. Für diese Anmeldung sind Kennzeichner-Typen weniger relevant.

[0044] Bei der Angabe eines speziellen Falls von NAT, beispielsweise in einer IP-Sec-Strategie-Datenbank, trifft der Benutzer eine Ja/Nein-Entscheidung, z. B. in einem Kontrollkästchen. Wie hier verwendet, bezieht sich eine IP-Sec-Strategie auf die vollständige Anzahl von konfigurierten IP-Sec-Informationen über ein System. Diese Informationen werden in einer Datenbank gespeichert, die als IP-Sec-Datenbank oder IP-Sec-Strategie-Datenbank bezeichnet wird. Beantworter-Modus-NAT-Merker IDci und IDcr können Teil der Verbindungsdefinition sein. Der Initiator-Modus-Merker kann ein Teil des Benutzer-Clientpaars sein, das (nur) mit einer "lokalen Client-Kennung" verknüpft ist. Die Beantworter-NAT-Merker IDci und IDcr können unabhängig voneinander gesetzt werden. Beide sind nur relevant, wenn die Verbindungsdefinition einen externen Initialisierungsmodus aufweist.

[0045] In allen Fällen, in denen bis jetzt der NAT-Merker "gesetzt" war, war es erforderlich, dass der entsprechende Granularitätswert in der Verbindungsdefinition "s" (Skalar) war. Gemäß der vorliegenden Erfindung besteht diese Beschränkung bei dynamischer VPN-NAT nicht mehr. Das heißt, die Granularitäten "s" (Skalar), "f" (Filter) und "c" (Client) werden alle unterstützt. "Granularität" wird in RF02401, oben, auf den Seiten 15–16 beschrieben. Gemäß einer beispielhaften Ausführungsform der Erfindung, beispielsweise dem IBM AS/400, wird "Granularität" folgendermaßen umgesetzt: jede VPN-Verbindung besitzt fünf Wähler (selectors) (Felder in einem Datagramm, das eventuell geprüft wird, um festzustellen, ob in der VPN-Verbindung Verkehr vorhanden sein sollte; dies sind: Quelle-IP, Ziel-IP, Quellenanschluss, Zielanschluss und Protokoll. Gemäß dieser beispielhaften Ausführungsform erhält jeder Wähler (selector) beim Start einer VPN-Verbindung seinen Wert entweder (1) vom Strategiefilter für diese VPN-Verbindung (für Wähler-Granularität "f"), (2) einzelnen Werten von IKE (für Wähler-Granularität "s") oder (3) einem zusammenhängenden Bereich von Werten von IKE (für Wähler-Granularität "c").

[0046] In Bezug auf **Fig. 2** veranschaulicht das System einer beispielhaften Ausführungsform der vorliegenden Erfindung eine mögliche Kunden-Konfiguration, die Typ "b Ziel-aus" enthält. Die Netzwerke **462** und **466** werden durch

VPN-Gateway A 470 und VPN-Gateway B 472 über Netzwerk **460** verbunden. VPN-Gateway A 470 enthält in dieser Ausführungsform einen Domänennamen-Server (DNS) **468** und Tabelle **480**, die von Gateway **470** verwendet wird, um für externe Adressen die gleichen Aliasnamen bereitzustellen wie die auf ihrem eigenen Teilnetz **462** vorhandenen. (DNS **468** kann sich innerhalb von Gateway **470** oder auf einem Host **474** an anderer Stelle innerhalb von Netzwerk **462** hinter Gateway **470** in Bezug auf Tunnel **482** befinden.) Der Aliasnamen (beispielsweise 10.90.5.37) wird durch Gateway **470** unmittelbar vor IP sec in seine richtige, am anderen Ende von Tunnel **482** durch Gateway **472** verwendete Adresse übersetzt. Die Adressen, die für die vom Ziel ausgehende VPN-NAT verwendet werden, werden auf eine andere Art erhalten als für die anderen drei VPN-NAT-Typen. Das heißt, gemäß der vorliegenden Erfindung kann ein Kunde in Verbindung mit jedem fernen VPN-Gateway **472**, mit dem ein gegebenes Netzwerk **462** kommunizieren muss, eine Vorlage oder Übersetzungsregel einer vom Ziel ausgehenden VPN-NAT konfigurieren. Beispielsweise könnte die in Tabelle **480** dargestellte Regel wie folgt ausgedrückt werden: 10.5.*.*, was bedeutet, dass alle Adressen im angezeigten Teilnetz übersetzt werden. Die Ziel-aus-NAT-Regel kann eine einzelne IP-Adresse oder mehrere IP-Adressen in unterschiedlichen Formen als einen Bereich, ein Teilnetz, eine Liste oder als eine Kombination von diesen angeben.

[0047] Domänennamen-Server (DNS) **468** wird dazu konfiguriert, redundante Kopien von Informationen zu vermeiden, die im DNS-Server **468** (konfiguriert) enthalten sind. Diese Verwendung von DNS löst auch einfach das Problem, wie sowohl der Host **474** als auch VPN-Gateway **470** Informationen (durch Verwendung des vorhandenen DNS-Protokolls) gemeinsam nutzen können. DNS-Server **468** wird für externe Hosts in Intranets konfiguriert (wie beispielsweise Netzwerk B 466), bei denen IP-Adressen mit Netzwerk A 462 in Konflikt stehen oder stehen könnten. Die logischen Informationen in Tabelle **469** werden in DNS **468** konfiguriert: ein Hostname und zwei IP-Adressen. Die erste IP-Adresse **467** wird durch die DNS **468** für eine normale "gethostbyname()"-Abfrage (Typ A-Eintrag) zurückgegeben. Die zweite IP-Adresse **471** wird durch eine andere Abfrage zurückgegeben, vielleicht unter Verwendung von Texteinträgen der DNS. (Tabelle **480** in **Fig.** 2 ist logisch das Gleiche wie Tabelle **410** in **Fig.** 6.) Die Beziehung zwischen Tabelle **469** in **Fig.** 2 und Tabelle **410**, **480** ist folgendermaßen: IP-Adr1 **467** in Tabelle **469** bilden zusammen die lks von Tabelle **410**, **480**, und IP-Adr2 **471** bilden zusammen die rts von Tabelle **410**, **480**.

[0048] Gateway **470** und alle Hosts **474** hinter dem Gateway greifen alle über normale DNS-Abfragen auf Tabelle **469** zu. Hosts führen eine normale A-Eintrag-Suche durch (beispielsweise unter Verwendung von gethostbyname()) und erhalten IPaddr1 **467**. VPN-Gateway **470** führt eine Abfrage für IPaddr2 **471** durch, die beispielsweise im DNS-Texteintrag sein kann.

[0049] Um den DNS-Server **468** mit entsprechenden Informationen zu konfigurieren, kann einem Benutzer eine grafische Benutzeroberfläche zur Verfügung gestellt werden, in der logisch organisierte Informationen in Tabelle **469** direkt durch den Benutzer bereitgestellt werden können. Diese Informationen können dann in der grafischen Benutzeroberfläche (GUI) verwendet werden, um die entsprechenden DNS-Einträge zu aktualisieren. Im Allgemeinen würde für jeden Host mit folgenden Merkmalen ein Eintrag gemacht werden: er ist außerhalb von Netzwerk A **462**, er ist außerhalb des Intranets **466**, die Adressen in **462** und **466** könnten miteinander in Konflikt stehen, zwischen Netzwerk **462** und **466** wird eine VPN-Verbindung benutzt, aus geschäftlichen Gründen müssen Hosts in Netzwerk **462** mit einem bestimmten Host in Netzwerk **466** kommunizieren. Somit wird der DNS-Server **468** gemäß der bevorzugten Ausführungsform der Erfindung auf eine neue und vorteilhafte Weise verwendet, die jedoch von seiner aktuellen Funktionalität unterstützt wird. Das heißt, dass diese neue Verwendung von DNS **458** das Problem löst, wie Tabelle **410**, **480** (insbesondere die lks-Spalte) in allen Hosts im Netzwerk **462** und VPN-Gateway **470** konsistent ist. Dieses Problem muss gelöst werden, da jeder Host, z. B. **474**, der mit einem der externen Hosts kommunizieren möchte, z. B. mit **476**, die lks-Adresse des externen Hosts kennen muss. Und der VPN-Gateway **470** muss auch für einen gegebenen Host **476** die gleiche lks-Adresse kennen. DNS **468** wird verwendet, um das Problem der Verteilung allgemeiner Informationen ohne mehrere Kopien und ohne die Probleme, die mit der Aufrechterhaltung des Umlaufs mehrerer Kopien verknüpft sind, zu lösen.

[0050] Die Art, in der VPN-NAT-IP-Pools mit Netzwerk-Szenarios für die anderen drei Typen – "a Quelle-aus", "c Quelle-ein" und "d Ziel-ein" zusammenhängen, wird in der anhängigen Patenanmeldung Seriennummer 09/578,215, eingereicht am 23.05.99 gezeigt. Für Typ "b Ziel-aus" ist der Satz von IPaddrl **467** (die gesamte Spalte in Tabelle **469**) das logische Äquivalent für die NAT-Pools der anderen drei Typen. Wie in Tabelle **469** konfiguriert, wird der Pool statisch den rts zugeordnet. In den anderen drei Typen wird der Pool dynamisch zugeordnet, wenn Verkehr stattfindet. Anders ausgedrückt, die Bindungszeit eines lks mit einem rts ist für Typ "b Ziel-aus" die Zeit, in der ein Paar in der DNS konfiguriert wird, wobei diese Bindung bis zu einer Neukonfiguration bestehen bleibt. Die Bindungszeit eines lks mit einem rts für die anderen Typen der NAT ist die Zeit, in der sich Verkehr stattfindet, der die Durchführung von NAT erfordert, wobei die Bindung für die Dauer des Verkehrs bestehen bleibt.

[0051] Wieder bezugnehmend auf **Fig.** 1 definiert der Benutzer in Schritt **22** eine Anzahl von IP-Adressen, die für die ausschließliche Verwendung der VPN-NAT-Funktion verfügbar sind. Jeder Pool ist vorzugsweise als ein Bereich der IP-Adresse definierbar, könnte aber auch aus einer Liste zusammenhängender Adressen bestehen und ist natürlich mit den Einheiten der Strategie-Datenbank ferner und lokaler Kennungs-IP-Sec (remote ID and local ID Ip Sec Policy database entities) verknüpft.

[0052] Wieder bezugnehmend auf **Fig.** 1 werden in Schritt **24** die Verbindungen im Initiator-Modus gestartet. Wie im Zusammenhang mit **Fig.** 5 nachfolgend ausführlicher beschrieben wird, überprüft der Verbindungsmanager **300** (**Fig.** 5) beim Starten einer Verbindung im Initiator-Modus den Merker do **313** in der VPN-Strategie-Datenbank **304**, um festzustellen, ob die lokale Client-Kennung übersetzt werden muss. Weiterhin bezugnehmend auf **Fig.** 5 erzeugt der Verbindungsmanager **300** die Laufzeit-Zuordnungstabelle **480** in **Fig.** 2, wenn Ziel-aus-NAT auf eine lokal gestartete VPN-Verbindung anzuwenden ist. Dies geschieht folgendermaßen: für jede IP-Adresse, die (als Bereich, Liste, Teilnetz oder einer Kombination) als eine Zieladresse für die VPN-Verbindung definiert ist, führt der Verbindungsmanager **300** eine DNS-Suche (beispielsweise nach dem Texteintrag) für diese Zieladresse durch, um die rts-Adresse zu erhalten. Die Zieladresse entspricht IPaddr1 467 und die von der DNS-Abfrage zurückgegebene Adresse entspricht IPaddr2 **471** in Tabelle **469** (**Fig.** 2). IPaddr2 **471** kann eine global routingfähige Adresse (routable address) oder eine private (z. B. 10.*.*.*) Adresse sein. Für eine lokal gestartete VPN-Verbindung fordert der Verbindungsmanager **300** an, dass IKE **330** (**Fig.** 5) Sicher-

heitszuordnungen (security associations) oder SA-Paare (SAs) unter Verwendung der rts-Adresse aushandelt. Nachdem IKE die SAs fertiggestellt hat, werden sie in der Startmeldung **332** an den Verbindungsmanager weitergegeben. Für eine ferngestartete Verbindung werden die SAs auf die gleiche Art weitergegeben.

[0053] Die NAT-rts-IP-Adresse wird dem Sicherheitszuordnungs-(security association)(SA)Paar hinzugefügt, das durch die vom IKE zurückgegebenen SAs fertiggestellt wird. Der Verbindungsmanager lädt dann die Verbindung zur IP-Sec. Ein SA-Paar besteht aus zwei Sicherheitszuordnungen (security associations) (definiert durch RFC2401, oben), eine eingehende und eine ausgehende.

[0054] IPSec erzeugt NAT-Regeln für die beiden SAs. Bei Ausgang erfolgt NAT nach der Filterung und vor IPSec, bei Eingang erfolgt NAT nach IPSec (und vor der Filterung, wenn überhaupt). In diesem Sinne "wickelt" NAT den lokalen Verbindungsendpunkt (connection endpoint) der IPSec-Verbindung "ein". In Bezug auf die **Fig.** 3 und 4 werden konventionelle NAT-Funktionen als Hintergrund und Kontrast für spätere Figuren veranschaulicht, die VPN-NAT-Typen gemäß der Erfindung zeigen.

[0055] In Bezug auf **Fig.** 3 ist die einfachste Form von NAT statisch. Die beiden konventionellen NAT-Typen werden ausdrücklich vom Benutzer durch Schreiben der entsprechenden NAT-Regel-Anweisungen über die OpNat-GUI konfiguriert. Dies steht im Gegensatz zu IPSec-NAT, in der die tatsächlichen NAT-Regeln oder Anweisungen durch das System erzeugt werden. Die ZUORDNEN-Anweisung <ORDNE lks ZU rts ZU> von **Fig.** 3 und die VERBERGEN-Anweisung <ip-adr-Satz HINTER rts VERBERGEN> von **Fig.** 4 sind solche NAT-Regel-Anweisungen.

[0056] Wieder in Bezug auf **Fig.** 3 wird, wenn bei ausgehender Verarbeitung in Schritt <1> die Quelle-IP **70** mit lks **72** in der Anweisung "ORDNE lks ZU rts ZU" übereinstimmt, in Schritt <2> Quell-ip **70** in rts **76** übersetzt. Wenn bei eingehender Verarbeitung in Schritt <3> Ziel-ip **74** mit rts **76** übereinstimmt, wird in Schritt <4> Ziel-ip **74** in lks **72** übersetzt. (Schritte <1>, <2>. . . beziehen sich auf die eingekreisten Nummern 1, 2. . . in den Figuren.)

[0057] In Bezug auf **Fig.** 4 verwendet Maskeraden-NAT (auch als Netzwerkadressen- und Anschluss-Übersetzung (NAPT) bezeichnet) die VERBERGEN-Anweisung oben und liefert Vielezu-Eine-Adressenübersetzung unter Verwendung ihrer eigenen Anschlusspools **118** (UDP, TCP), um daran erinnert zu werden, wie der eingehende Verkehr zu übersetzen ist. Im Gegensatz zu statischer NAT (**Fig.** 3) können Maskeraden-NAT-Konversationen <KONVERSATION Quell-ip, Quell-Anschluss, rtsip, rts-Anschluss, . . .> nur durch interne (lks) Adressen gestartet werden. Einige VPN-NAT-Typen setzen auch Anschlusszuordnung ein, um mehreren lokalen Hosts die gleichzeitige Kommunikation mit dem externen System über die selbe VPN-Verbindung zu ermöglichen.

[0058] Wenn, wieder in Bezug auf **Fig.** 4, bei der Verarbeitung ausgehender Datagramme in Schritt <1> ermittelt wird, dass die Quelle-IP-Adresse **90** im IP-Adressensatz **92** der VERBERGEN-Anweisung sein soll, wird in Schritt <2> die KONVERSATION durch Kopieren von Quell-ip90 in das KONVERSATION-Feld **94**, in Schritt <3> durch Kopieren des Quellenanschlusses **98** in das Feld **96**, in Schritt <4> durch Kopieren von rts **104** in das Feld **100** und in Schritt <5> durch Kopieren des rts-Anschlusses in das Feld **102** aus dem richtigen Pool des Anschlusspools **118** eingerichtet.

[0059] Anschließend wird in Schritt <6> Quelle-IP **90** in rts **104** übersetzt, und in Schritt <7> wird Quellenanschluss **98** in rts-Anschluss **102** umgeändert. Wenn bei der Verarbeitung eingehender Datagramme in Schritt <8> Ziel-IP-Adresse **106** und Zielanschluss **108** den KONVERSATION-Feldern rtsip **100** bzw. rts-Anschluss **102** entsprechen, wird in Schritt <9> Ziel-IP-Adresse **106** in KONVERSATION-Quelle-IP-Adresse **94** und in Schritt <10> Zielanschluss **108** in KONVERSATION-Quellenanschluss **96** übersetzt.

[0060] Einige spezielle Situationen werden ebenfalls durch NAT bewältigt. Dazu gehört die Bewältigung spezieller Situationen, die durch FTP oder ICMP geschaffen werden, die beide die IP-Adressen enthalten, die übersetzt werden. (FTP bezieht sich auf File Transfer Protocol (Protokoll zur Übertragung von Dateien im Internet) und ist in RFC959 definiert. ICMP bezieht sich auf Internet Control Message Protocol (Internet-Steuernachrichtenprotokoll) und ist in RFC792 definiert). Neuberechnung der Prüfsumme wird durchgeführt. Sobald in der Maskeraden-NAT eine Konversation stattfindet, werden statt der ursprünglichen (ausscheidenden) VERBERGEN-Regel später Datagramme auf Übereinstimmung geprüft, werden die Anschlusspools verwaltet, wird die Dauer der Konversationen gemessen, werden die Konversationen selbst beendet und die Anschlüsse zugeordnet. Es ist ein besonderer Vorteil der Erfindung, dass ICMP und FTP (einschließlich der berühmten FTP-ANSCHLUSS- und PASV-Befehle und der Begleitprobleme) von VPN-NAT unterstützt werden.

[0061] Gemäß der vorliegenden Erfindung werden dynamisch bestimmte VPN-NAT-Regeln wie folgt umgesetzt. Der Kunde gibt über eine grafische Benutzeroberfläche (GUI) an, dass VPN-NAT durchgeführt werden soll. Mehrere IP-Adressen sind für die Quelle-IP-Adresse von lokal gestarteten Verbindungen erlaubt. Diese Mehrfach-IP-Adressen werden über einen (zusammenhängenden) Bereich oder über Adresse und Maske oder eine Adressenliste oder eine Kombination dieser Adressendarstellungen angegeben. Diese bilden den linksseitigen (lks) Adressensatz der VPN-NAT-Regel.

[0062] In **Fig.** 6 wird VPN-NAT-Ziel-aus veranschaulicht. Da eine Ziel-aus-NAT angefordert wird, wird für eine lokal gestartete Konversation in Schritt <-2> die implizite ZUORDNEN-Regel **428** durch eine Anzahl von DNS-Abfragen erstellt. Für jede lks-<-2>-Adresse wird eine Abfrage durchgeführt, um die entsprechende rts-<-1>-Adresse abzurufen. Es gibt wichtige Eigenschäften, die all diese Adressen gemeinsam haben: (a) sie sind im internen Netzwerk **462** (**Fig.** 2) des VPN-Gateway und zum VPN-Gateway routingfähig (routable to) und (b) sie werden innerhalb des internen Netzwerks für keinen anderen Zweck benötigt. Schritt <0> ist Teil des Starts der VPN-Verbindung und erfolgt während der Schritte **24** und **26** (**Fig.** 1). Nachdem die IKE-Verhandlung unter Verwendung von rts **424** abgeschlossen ist, wird in Schritt <0> die implizite ZUORDNEN-Regel in den Betriebssystemkernel geladen. Dieser Schritt <0> umfasst die folgenden Schritte; Laden der Verbindungs-SAs und Verbindungsfilter und Erstellung einer leeren Version von Tabelle **410**. Für ausgehende Verarbeitung wird in Schritt <1> die Ziel-IP-Adresse **434** des ausgehenden Datagramms mit dem lks-Eintrag **436** in der lokalen Bindungstabelle **410** verglichen. Wenn keine Übereinstimmung gefunden wird, ist kein Ziel-aus-NAT nötig. Wenn in Schritt <2> eine Übereinstimmung gefunden wird, wird die Datagramm-Ziel-IP-Adresse **434** durch rts **438** des Eintrags (Zeile, Paar, Regel sind äquivalente Begriffe) ersetzt, der die übereinstimmende lks **436** enthält. Die ausgehende NAT-Verarbeitung ist abgeschlossen und das Datagramm geht zum nächsten Schritt in der ausgehenden Verarbeitung, d. h. zu IP-Sec, über. Nach Verarbeitung eingehender IP-Sec wird in Schritt <3> für eingehende Verarbeitung

die Quellen-IP-Adresse **442** mit rts-Eintrag **438** in der lokalen Bindungstabelle **410** verglichen. Wenn keine Übereinstimmung gefunden wird, ist NAT nicht nötig. Wenn in Schritt <4> eine Übereinstimmung gefunden wird, wird die Quelle-IP-Adresse **442** durch die lks **436** des Eintrags ersetzt, der die übereinstimmende rts **438** enthält. Die eingehende NAT-Verarbeitung ist abgeschlossen und das Datagramm geht zum nächsten Schritt über, in dem gewöhnlich TCP/IP-Protokoll-Stapelverarbeitung (TCP/IP protocol stake processing) durchgeführt wird.

[0063] "Eingehend" ist die Abkürzung für "eingehendes Datagramm". Datagramme strömen aus dem VPN-Gateway (bekannt als "ausgehender Verkehr") und in den VPN-Gateway (bekannt als "eingehender Verkehr"). Diese beiden Richtungen oder Begriffe sind in nahezu allen Kommunikationen, wenn nicht in allen Fällen grundlegend, einschließlich in diskreten protokollbasierten Kommunikationen wie TCP/IP und folglich in allen Funktionen, die mit VPN-NAT verbunden sind.

[0064] Als Nächstes erfolgt das Laden zur IPSec. Bei Verarbeitung von ferngestartetem Verbindungsverkehr können für jedes eingehende und ausgehende Paket (Quelle und Ziel) zwei Adressenübersetzungen erfolgen.

[0065] In Bezug auf **Fig.** 5, schaut der Verbindungsmanagerserver **300** bei Empfang der Startmeldung (msg) **332** vom IKE-Server **330** auf die Verbindungsdefinition **306** in der Datenbank **304** und prüft die NAT-Merker **314**. Vor der Startmeldung **332** vom IKE-Server **330** an den Verbindungsmanager **300** geht eine Startmeldung **332** vom Verbindungsmanager **300** an den IKE **330** für lokal gestartete Verbindungen und nicht für ferngestartete Meldungen. In beiden Fällen ist die Startmeldung **332** von IKE **330** an den Verbindungsmanager **300** die gleiche Meldung. Wenn ein oder mehrere NAT-Fern-Merker Quelle-aus (qa) **308**, Quelle-ein (qe) **310**, Ziel-ein (ze) **312** oder Ziel-aus (za) **313** gesetzt ist, werden eine oder mehrere IP-Adressen vom entsprechenden NAT-Pool oder vom DNS **468** (**Fig.** 2) erhalten.

[0066] Wenn der Verbindungsmanager **300** bezüglich **Fig.** 5 in Verbindung mit **Fig.** 1 in Schritt **28** SA-Paar-Aktualisierungen **302** erhält, kopiert er die neuen SA-Paar-Informationen in die SA-Paar-Tabelle **322** im Verbindungsprozessspeicher **320**.

[0067] In Schritt **30** gibt der Verbindungsmanager **300** bei Beendigung einer Verbindung **34**, **36** jede NAT-IP-Adresse **52**, **54** frei (macht sie verfügbar), die mit der Verbindung verknüpft ist. NAT-IP-Adressen werden von der entsprechenden Liste **316** gelöscht, die vom Verbindungsmanager **300** unterhalten wird.

[0068] In **Fig.** 7 wird die Beziehung zwischen Adressendomänen und Hostadressen gezeigt, und es wird gezeigt, ob Ziel-aus-NAT und Quelle-aus-NAT erforderlich sind. Jeder Kreis stellt eine Adressendomäne dar – A stellt die Adresse eines Hosts **474** hinter Gateway **470** und B die Adresse eines externen Hosts **476** dar. In Fall I ist weder die Adresse von Host A noch die von Host B innerhalb der Verknüpfung (join) ihrer jeweiligen Adressendomänen, so dass keine Netzwerkadressen-Übersetzung (NAT) erforderlich ist. In Fall II ist nur die Adresse von Fern-Host B innerhalb der Verknüpfung der Adressendomänen; daher ist Ziel-aus-NAT erforderlich und Quelle-aus-NAT nicht. In Fall III ist die Adresse von Host A innerhalb der Verknüpfung (join) der Adressendomänen, nicht jedoch die Adresse von Host B; daher ist Quelle-aus-NAT erforderlich und Ziel-aus-NAT nicht. In Fall IV sind die Adressen der Hosts A und B innerhalb der Verknüpfung (join) der Adressendomänen, wobei sowohl Quelle-aus-NAT als auch Ziel-aus-NAT erforderlich sind.

Vorteile gegenüber dem Stand der Technik

[0069] Es ist ein Vorteil der Erfindung, ein verbessertes und stark vereinfachtes System und Verfahren für die gleichzeitige Ausführung von Netzwerkadressen-Übersetzung (NAT) und IP-Sicherheit (IP-Sec) bereitzustellen.

[0070] Weiterhin ist es ein Vorteil der Erfindung, ein System und ein Verfahren zur Herabsetzung der erhöhten Wahrscheinlichkeit von IP-Adressenkonflikten bereitzustellen, die ein virtuelles privates Netzwerk (VPN) mit sich bringt.

[0071] Weiterhin ist es ein Vorteil der Erfindung, ein System und ein Verfahren für die Nutzung von VPNs bereitzustellen, ohne dass eine Neuadressierung einer Domäne (eine teure Alternative) erforderlich wird.

[0072] Weiterhin ist es ein Vorteil der Erfindung, ein System und ein Verfahren für VPN-NAT bereitzustellen, das vollständig im IP-Sec-Gateway erzielt wird, ohne dass Änderungen in Domänenhosts erforderlich werden.

[0073] Weiterhin ist es ein Vorteil der Erfindung, ein System und ein Verfahren für VPN-NAT bereitzustellen, das keine oder nur kleinere Änderungen am Routing in jeder verbundenen Domäne erfordert.

[0074] Weiterhin ist es ein Vorteil der Erfindung, ein System und ein Verfahren für VPN-NAT bereitzustellen, das einfach zu konfigurieren ist.

[0075] Weiterhin ist es ein Vorteil der Erfindung, eine Lösung für die Adressenkollisionsprobleme bereitzustellen, die von VPNs verursacht werden.

[0076] Weiterhin ist es ein Vorteil der Erfindung, eine vereinfachte Lösung für die Konfiguration von VPN-Verbindungen durch Kunden bereitzustellen.

[0077] Weiterhin ist es ein Vorteil der Erfindung, ein System und ein Verfahren bereitzustellen, das es einer einzelnen VPN-Verbindung ermöglicht, mehrere VPN-NAT-Regeln zu unterstützen.

[0078] Weiterhin ist es ein Vorteil der Erfindung, ein System und ein Verfahren bereitzustellen, das Konflikte unter den implizit oder dynamisch zugeordneten VPN-NAT-Regeln systemübergreifend vermeidet.

[0079] Weiterhin ist es ein Vorteil der Erfindung, ein System und ein Verfahren bereitzustellen, das die Systemverwaltungszeit in Systemen für dynamische NAT-Regeln durch Beseitigung der Notwendigkeit der Verwaltung zahlreicher einzelner VPN-Verbindungen für jede NAT-Regel verringert.

[0080] Weiterhin ist es ein Vorteil der Erfindung, ein VPN-NAT-System und -Verfahren bereitzustellen, das die Netzwerküberwachung und die Verkehrsanalyse vereinfacht.

[0081] Weiterhin ist es ein Vorteil der Erfindung, ein VPN-NAT-System und -Verfahren bereitzustellen, das die Netzwerküberwachung und die Verkehrsanalyse vereinfacht.

[0082] Weiterhin ist es ein Vorteil der Erfindung, ein ganzes VPN-NAT-Lösungspaket bereitzustellen, das dem Bedarf der Kunden entspricht.

[0083] Weiterhin ist es ein Vorteil der Erfindung, ein nichtredundantes Verfahren bereitzustellen, um Adressenverbindungen für bestimmte VPN-NAT-Typen zu konfigurieren und zu unterhalten.

[0084] Weiterhin ist es ein Vorteil der Erfindung, dass für alle VPN-NAT-Typen mehrere VPN-NAT-Regeln pro VPN-Verbindung angegeben werden können.

Alternative Ausführungsformen

[0085] Es ist klar, dass, obwohl spezielle Ausführungsformen der Erfindung hier zum Zweck der Veranschaulichung beschrieben worden sind, verschiedene Abänderungen durchgeführt werden können, ohne vom Geist und Rahmen der Erfindung abzuweichen. Insbesondere liegt es im Bereich der Erfindung, ein Computerprogrammprodukt oder -programmelement oder eine Programmspeicher- der Speichereinheit, wie beispielsweise ein festes oder flüssiges Übertragungsmedium, magnetischen oder optischen Draht, ein Band oder eine Platte oder Ähnliches zum Speichern von maschinenlesbaren Signalen zur Steuerung des Betriebs eines Computers nach dem Verfahren der Erfindung und/oder zur Strukturierung seiner Komponenten gemäß dem System der Erfindung bereitzustellen.

[0086] Weiterhin kann jeder Schritt des Verfahrens auf jedem gewöhnlichen Computer ausgeführt werden, beispielsweise auf einem IBM-System 390, AS/400, PC oder dergleichen und gemäß einem oder mehreren oder einem Teil von einem oder mehreren Programmelementen, -modulen oder -objekten, die von einer beliebigen Programmiersprache erzeugt wurden, wie beispielsweise C++, Java, P1/i, Fortran oder dergleichen. Und weiterhin kann jeder Schritt oder eine Datei oder ein Objekt oder dergleichen, die bzw. das jeden Schritt ausführt, durch Spezialhardware oder durch ein für diesen Zweck entwickeltes Schaltkreismodul ausgeführt werden.

[0087] Entsprechend ist der Rahmen des Schutzes dieser Erfindung nur durch folgende Ansprüche und ihre Äquivalente begrenzt.

Patentansprüche

1. Verfahren zur Integration von Netzwerkadressen-Übersetzung innerhalb eines gesicherten virtuellen privaten Netzwerks, das folgende Schritte umfasst:
Konfigurieren eines internen Netzwerkhosts, um ausgewählten Verkehr an eine Proxy-Netzwerkadresse zu senden;
Konfigurieren eines virtuellen privaten Netzwerk-Gateways mit einer Zuordnungstabelle von Netzwerkadressen-Übersetzungsregeln; und
Starten einer virtuellen privaten Netzwerkverbindung nach den Netzwerkadressen-Übersetzungsregeln.

2. Verfahren nach Anspruch 1, das weiterhin den Schritt der Konfiguration jeder Regel umfasst, um eine Zieladresse und eine Ersatzadresse einzuschließen.

3. Verfahren nach Anspruch 2, das weiterhin die Verwendung der virtuellen privaten Netzwerkverbindung gemäß folgender Schritte umfasst:
Erzeugen eines Datagramms am internen Netzwerkhost;
Weiterleiten des Datagramms zum Gateway;
Weiterleiten des Datagramms am Gateway durch Filterregeln, die einen virtuellen privaten Netzwerktunnel definieren;
Verarbeiten einer auf die Zuordnungstabelle zugreifenden Zieladresse im Datagramm beim virtuellen privaten Netzwerktunnel gemäß folgender Schritte:
Durchsuchen der Tabelle nach einer Übereinstimmung der Zieladresse mit einer linken Adresse eines linken/rechten Adressenpaars;
Durchführen einer Adressenübersetzung durch Ersetzen der Zieladresse durch die rechte Adresse des Adressenpaars, wenn eine Übereinstimmung gefunden wird; und
Durchführen einer Sicherheitsverarbeitung.

4. Verfahren nach Anspruch 3, das weiterhin folgende Schritte umfasst:
Empfang eines eingehenden Datagramms am Gateway von einem externen Host einschließlich eines Sicherheitsvermerks;
als Reaktion auf den Sicherheitsvermerk, Bestimmen einer Verbindungadresse der Netzwerkquelle;
Verarbeiten der Netzwerkverbindungsadresse gemäß folgender Schritte:
Durchsuchen der Tabelle nach Übereinstimmung der Quellenverbindungsadresse mit einer rechten Adresse;
wenn eine Übereinstimmung gefunden wird, Durchführen einer Adressenübersetzung durch Ersetzen der Quellenverbindungsadresse durch den linken Eintrag des Adressenpaars; und
Durchführen einer Sicherheitsverarbeitung.

5. Verfahren nach Anspruch 4, wobei der Schritt des Bestimmens den Erhalt einer lokal routingfähigen Host-Aliasadresse für den externen Host von einem Domänennamen-Server hinter dem Gateway beinhaltet.

6. Verfahren für die Bedienung von Domänennamen, das Folgendes umfasst:
Konfigurieren eines Domänennamen-Servers hinter einem Gateway, um lokal routingfähige Host-Aliasadressen für externe Hosts zu speichern;
Aufbau einer Zuordnungstabelle durch:
Anzeigen einer Liste mit Hostnamen, die die linksseitigen Adresseinträge bilden, für einen Benutzer;
Aufforderung des Benutzers zur Eingabe eines entsprechenden rechtseitigen Aliasadresseneintrags als Reaktion auf die Auswahl eines Eintrags in der Liste durch einen Benutzer;
Wiederholen der beiden Schritte des Anzeigens und der Aufforderung für eine Vielzahl von Zuordnungstabelleneinträgen;
Bedienen der Aliasadresse als Reaktion auf die Anforderung von einem Gateway oder einem Host hinter dem Gateway für eine rechtsseitige Adresse.

7. System zur Integration von Netzwerkadressen-Übersetzung innerhalb eines gesicherten virtuellen privaten Netzwerks, das Folgendes umfasst:

einen internen Netzwerkhost zum Senden von ausgewähltem Verkehr an eine Proxy-Netzwerkadresse;
eine Zuordnungstabelle mit Übersetzungsregeln von Netzwerkadressen; und
einen Gateway, der auf die Übersetzungsregeln von Netzwerkadressen zum Starten einer virtuellen privaten Netzwerkverbindung anspricht.

8. System nach Anspruch 7, wobei die Übersetzungsregeln für Netzwerkadressen eine Zieladresse und eine Ersatzadresse beinhalten.

9. System nach Anspruch 8, wobei der Gateway in der Lage ist, als Reaktion auf ein Datagramm vom Host das Weiterleiten des Datagramms durch Filterregeln, die einen virtuellen privaten Netzwerktunnel definieren, durchzuführen.

10. System nach Anspruch 9, das weiterhin umfasst:
Mittel für die Verarbeitung einer Zieladresse im Datagramm beim virtuellen privaten Netzwerktunnel, die auf die Zuordnungstabelle zugreifen kann.

11. System nach Anspruch 10, das weiterhin umfasst:
Mittel zum Durchsuchen der Tabelle nach einer Übereinstimmung der Zieladresse mit einer linken Adresse eines linken/rechten Adressenpaars;
Mittel, das in der Lage ist, eine Übereinstimmung für die Durchführung einer Adressenübersetzung durch Ersetzen der Zieladresse durch die rechte Adresse des Adressenpaars zu finden; und
Mittel zur Durchführung der Sicherheitsverarbeitung.

12. System nach Anspruch 9, das weiterhin umfasst:
Empfangen, einschließlich eines Sicherheitsvermerks;
Mittel, das auf den Sicherheitsvermerk reagiert, der am Gateway in einem eingehenden Datagramm von einem externen Host empfangen wird, um die Verbindungsadresse einer Netzwerkquelle zu ermitteln;
Mittel zum Verarbeiten der Netzwerkverbindungsadresse durch Durchsuchen der Tabelle nach einer Übereinstimmung der Quellenverbindungsadresse mit einer rechten Adresse, und wenn eine Übereinstimmung gefunden wird, Durchführen einer Adressenübersetzung durch Ersetzen der Quellenverbindungsadresse durch den linken Eintrag des Adressenpaars; und
Durchführen einer Sicherheitsverarbeitung.

13. System nach Anspruch 12, das weiterhin einen Domänenserver hinter dem Gateway umfasst, um sowohl den Gateway als auch den lokalen Host mit lokalen routingfähigen Host-Aliasadressen für den externen Host zu bedienen.

14. System zur Domänennamen-Bedienung, das Folgendes umfasst:
einen Domänennamen-Server hinter einem Gateway zum Speichern lokaler routingfähiger Host-Aliasadressen für externe Hosts;
Mittel zur Erzeugung einer Zuordnungstabelle, wobei einem Benutzer eine Liste mit Hostnamen angezeigt wird, die die linksseitigen Adresseinträge bilden und als Reaktion auf die Auswahl eines Eintrags in der Liste durch einen Benutzer dieser sich wiederholende Aufforderungen zur Eingabe eines entsprechenden rechtsseitigen Aliasadresseneintrags erhält; und
Mittel, das auf eine Anforderung von einem Gateway oder einem Host hinter dem Gateway für eine rechtsseitige Adresse für die Bedienung der Aliasadresse anspricht.

15. Prozess zur Durchführung von VPN-NAT-Ziel-aus, der folgende Schritte umfasst:
Erstellen einer lokalen Bindungstabelle mit Regeln, die rechtsseitige und linksseitige Regeleintragspaare enthalten;
als Reaktion auf eine lokal gestartete Konversation, Anfordern einer Netzwerkadressen-Übersetzung, Erstellen einer impliziten ZUORDNEN-Regel, die einen linken und einen rechten Eintrag enthält, durch Kopieren einer lokalen Client-Kennung in den linken Eintrag und durch Erhalt des rechten Eintrags von einem Adresspool erstellt;
Durchführen einer Sicherheitsverarbeitung mit Bezug auf den rechten Eintrag;
Starten einer VPN-Verbindung und Laden einer ersten impliziten Regel;
für ausgehende Verarbeitung, Vergleichen der Zieladresse mit dem linken Regeleintrag in der lokalen Bindungstabelle und, falls eine Übereinstimmung gefunden wird, Ersetzen der Zieladresse mit dem rechten Regeleintrag; und
für eingehende Verarbeitung, Vergleichen der Quellenadresse mit dem rechten Regeleintrag in der lokalen Bindungstabelle und, falls eine Übereinstimmung gefunden wird, Ersetzen der Quellenadresse mit dem linken Regeleintrag.

16. Programmspeichereinheit, die durch eine Maschine lesbar ist, die ein reales Programm mit Anweisungen enthält, die durch eine Maschine ausführbar sind, um die Verfahrensschritte zur Integration der Netzwerkadressen-Übersetzung innerhalb eines gesicherten virtuellen privaten Netzwerks durchzuführen, wobei das Verfahren folgende Schritte umfasst:
Konfiguration eines internen Netzwerkhosts, um ausgewählten Verkehr an eine Proxy-Netzwerkadresse zu senden;
Konfigurieren eines virtuellen privaten Netzwerk-Gateways mit einer Zuordnungstabelle, die Netzwerkadressen-Übersetzungsregeln enthält;
Starten einer virtuellen privaten Netzwerkverbindung nach den Netzwerkadressen-Übersetzungsregeln.

17. Maschinenlesbare Programmspeichereinheit, die ein reales Programm mit Anweisungen enthält, die von einer Maschine ausgeführt werden können, um Verfahrensschritte zum Bedienen von Domänennamen durchzuführen, wobei das Verfahren folgende Schritte umfasst:
Konfigurieren eines Domänennamen-Servers hinter einem Gateway, um lokal routingfähige Host-Aliasadressen für externe Hosts zu speichern;
Aufbau einer Zuordnungstabelle durch:
Anzeigen einer Liste mit Hostnamen, die die linksseitigen Adresseinträge bilden, für einen Benutzer;
als Reaktion auf die Auswahl eines Eintrags in der Liste durch einen Benutzer, Auffordern des Benutzers zur Eingabe eines entsprechenden rechtseitigen Aliasadresseintrags;

Wiederholen der beiden Schritte des Anzeigens und Aufforderns für eine Vielzahl von Zuordnungstabelleneinträgen;
als Reaktion auf eine Anforderung von einem Gateway oder einem Host hinter dem Gateway für eine rechtsseitige Adresse, Bedienen der Aliasadresse.

18. Maschinenlesbare Programmspeichereinheit, die ein reales Programm mit Anweisungen enthält, die von einer Maschine ausgeführt werden können, um Verfahrensschritte zur Durchführung von VPN-NAT-Ziel-aus durchzuführen, wobei das Verfahren folgende Schritte umfasst:
Erstellen einer lokalen Bindungsregeltabelle, die rechtsseitige und linksseitige Regeleintragspaare enthält;
als Reaktion auf eine lokal gestartete Konversation, Anfordern einer Netzwerkadressen-Übersetzung, Erstellen einer impliziten ZUORDNEN-Regel, die einen linken und einen rechten Eintrag enthält, durch Kopieren einer lokalen Client-Kennung in den linken Eintrag und durch Erhalt des rechten Eintrags von einem Adresspool erstellt;
Durchführen einer Sicherheitsverarbeitung mit Bezug auf den rechten Eintrag;
Starten einer VPN-Verbindung einschließlich des Ladens einer ersten impliziten Regel;
für ausgehende Verarbeitung, Vergleichen der Zieladresse mit dem linken Regeleintrag in der lokalen Bindungstabelle und, falls eine Übereinstimmung gefunden wird, Ersetzen der Zieladresse mit dem rechten Regeleintrag; und
für eingehende Verarbeitung, Vergleichen der Quellenadresse mit dem rechten Regeleintrag in der lokalen Bindungstabelle und, falls eine Übereinstimmung gefunden wird, Ersetzen der Quellenadresse durch den linken Regeleintrag.

19. Ein Herstellungsartikel, der Folgendes umfasst: ein durch einen Computer verwendbares Medium, das ein computerlesbares Programmcodemittel zur Bedienung von Domänennamen enthält, wobei das computerlesbare Programmmittel in dem Herstellungsartikel Folgendes umfasst:
computerlesbares Programmcodemittel, das bewirkt, dass ein Computer das Speichern lokal routingfähiger Host-Aliasadressen für externe Hosts durchführt;
computerlesbares Programmcodemittel für die Erzeugung einer Zuordnungstabelle, wobei für einen Benutzer eine Liste mit Hostnamen angezeigt wird, die die linksseitigen Adresseinträge bilden, und als Reaktion auf die Auswahl eines Eintrags in der Liste durch einen Benutzer, wiederkehrende Aufforderungen des Benutzers zur Eingabe eines entsprechenden rechtsseitigen Aliasadresseintrags; und
computerlesbares Programmcodemittel, das auf eine Anforderung von einem Gateway oder einem Host hinter dem Gateway für eine rechtsseitige Adresse für die Bedienung der Aliasadresse anspricht.

Hierzu 7 Seite(n) Zeichnungen

Nummer: DE 101 28 493 A1
Int. Cl.[7]: H 04 L 12/46
Offenlegungstag: 3. Januar 2002

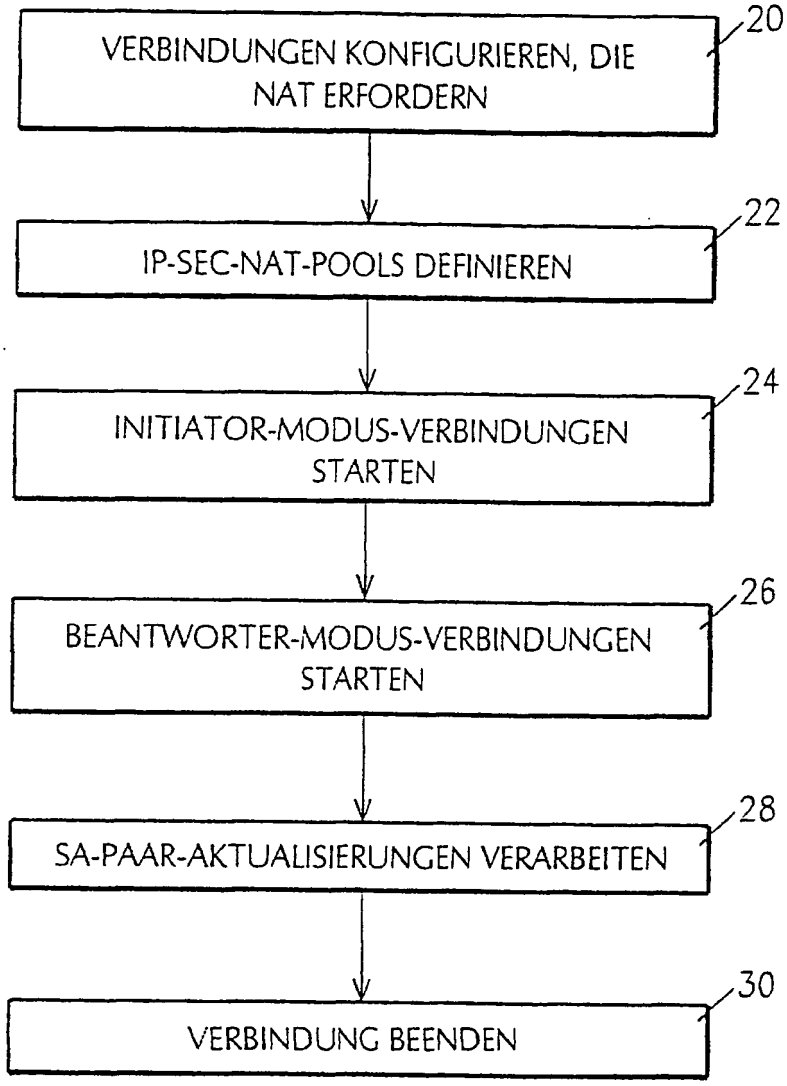


FIG. 1

Nummer: DE 101 28 493 A1
Int. Cl.[7]: H 04 L 12/46
Offenlegungstag: 3. Januar 2002

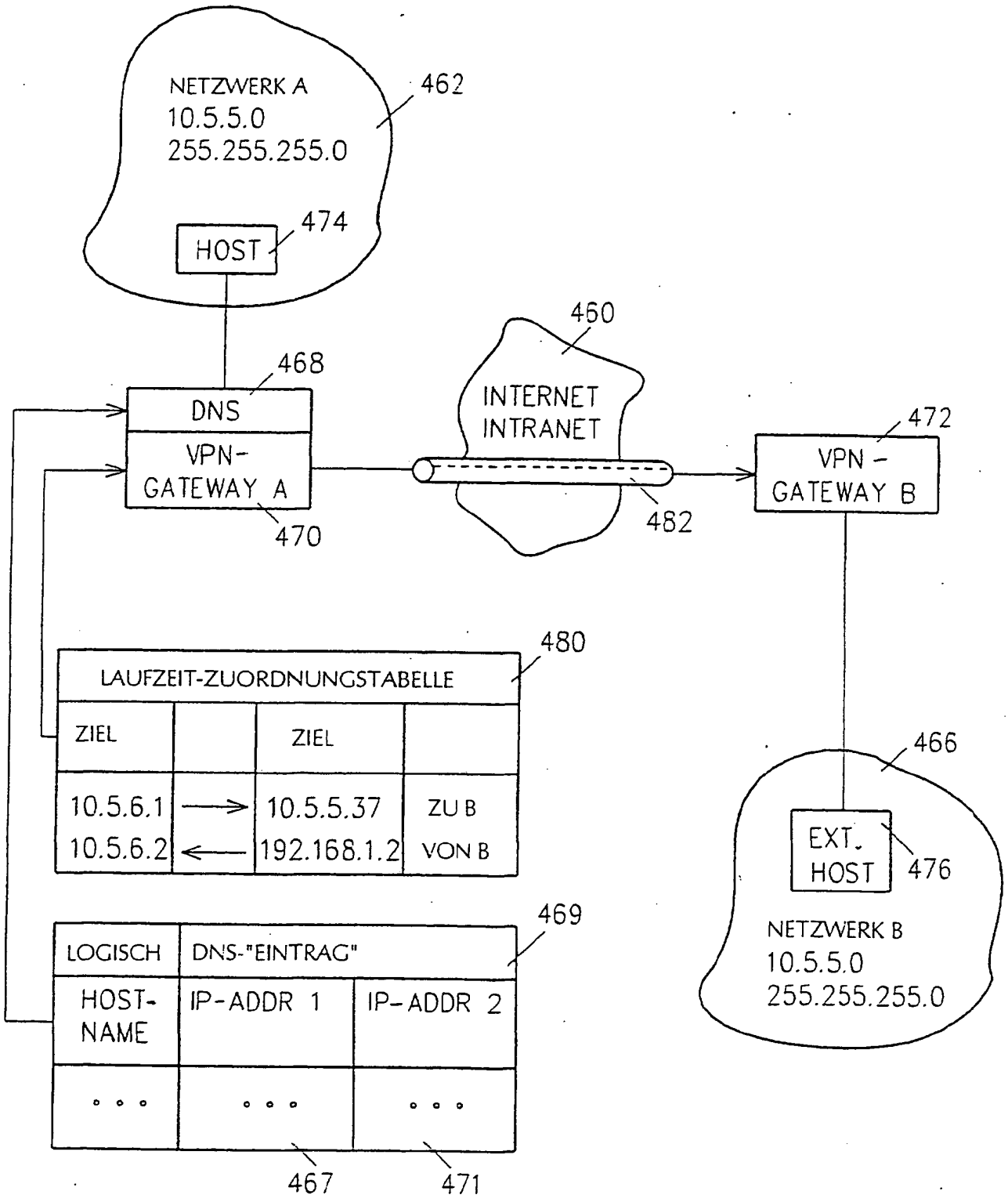


FIG. 2

Nummer: DE 101 28 493 A1
Int. Cl.[7]: H 04 L 12/46
Offenlegungstag: 3. Januar 2002

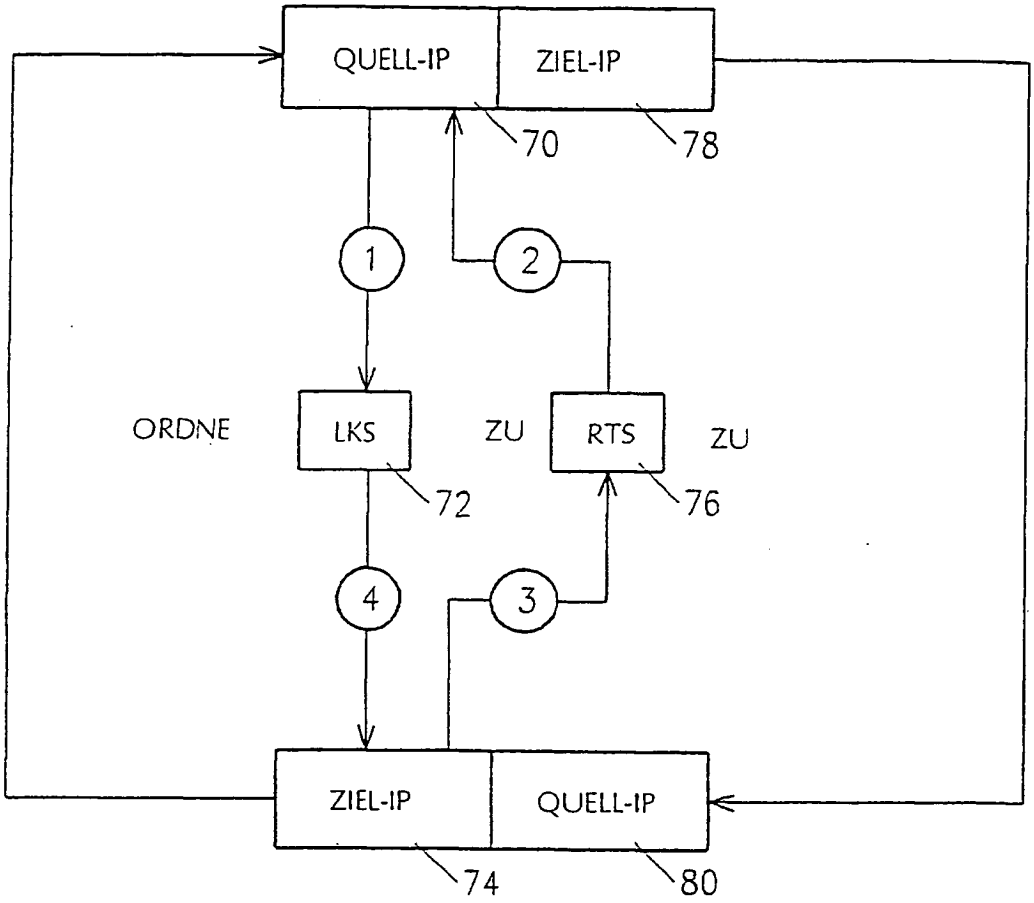


FIG. 3

Nummer: DE 101 28 493 A1
Int. Cl.[7]: H 04 L 12/46
Offenlegungstag: 3. Januar 2002

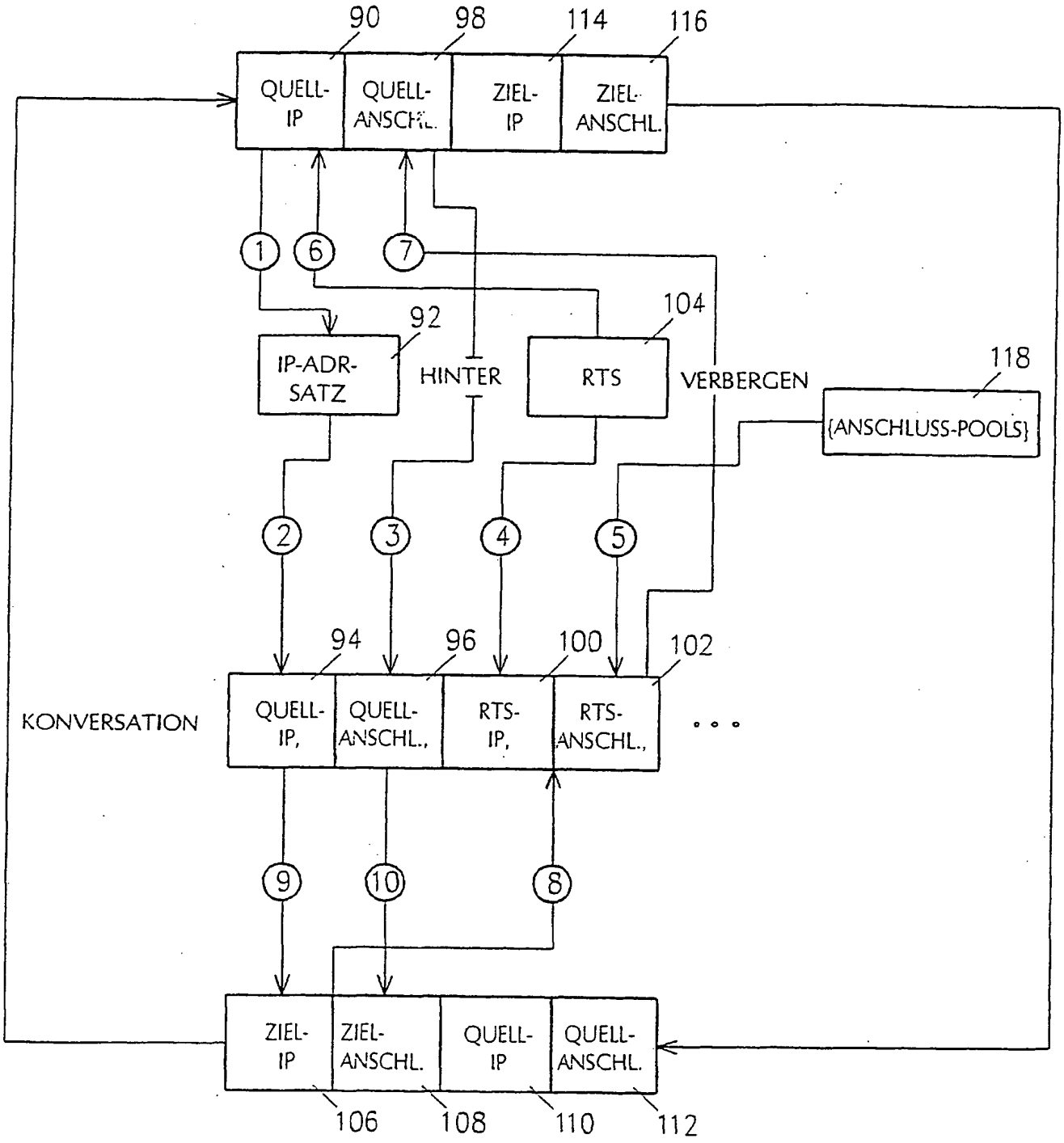


FIG. 4

Nummer: DE 101 28 493 A1
Int. Cl.[7]: H 04 L 12/46
Offenlegungstag: 3. Januar 2002

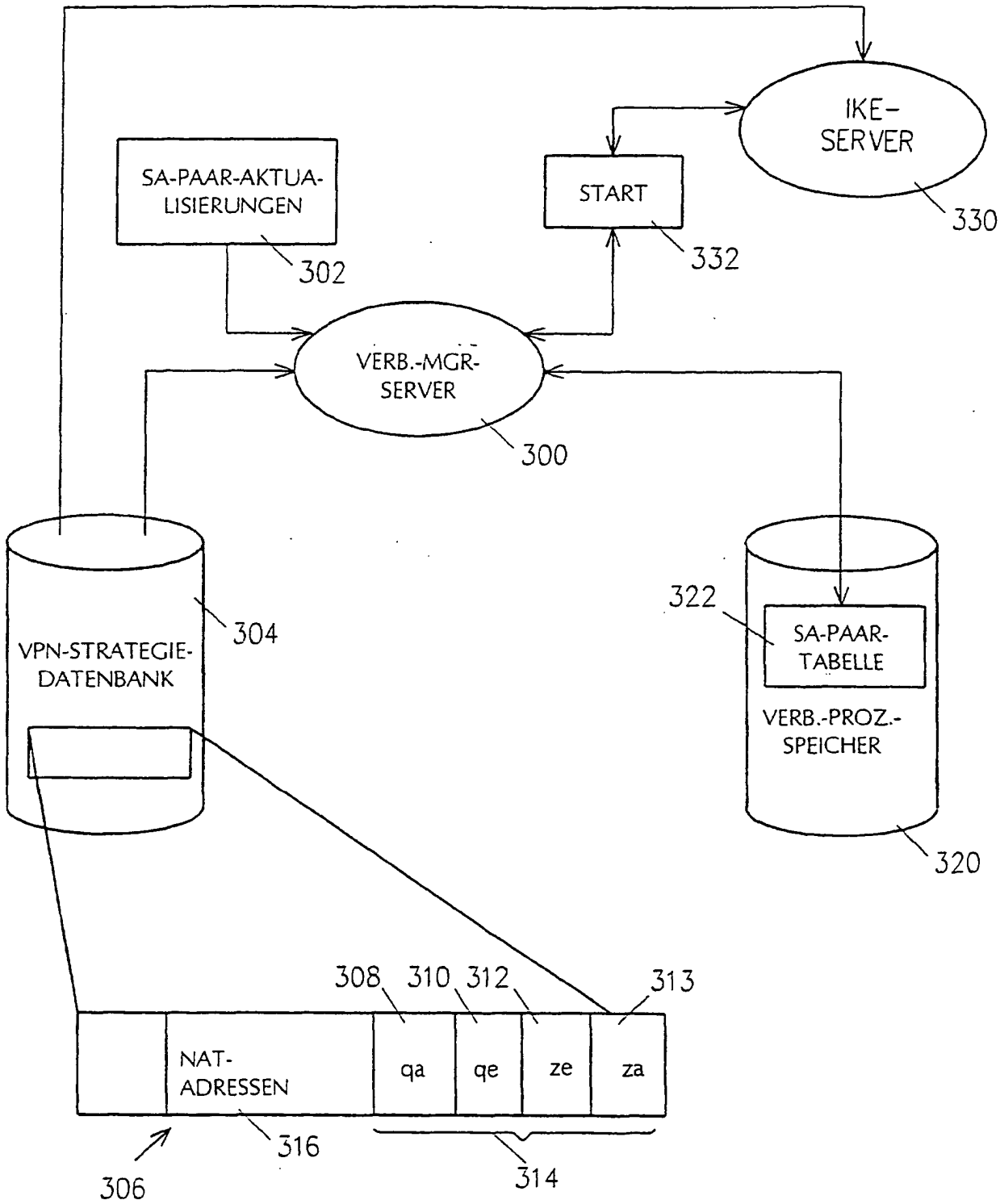


FIG. 5

Nummer: DE 101 28 493 A1
Int. Cl.[7]: H 04 L 12/46
Offenlegungstag: 3. Januar 2002

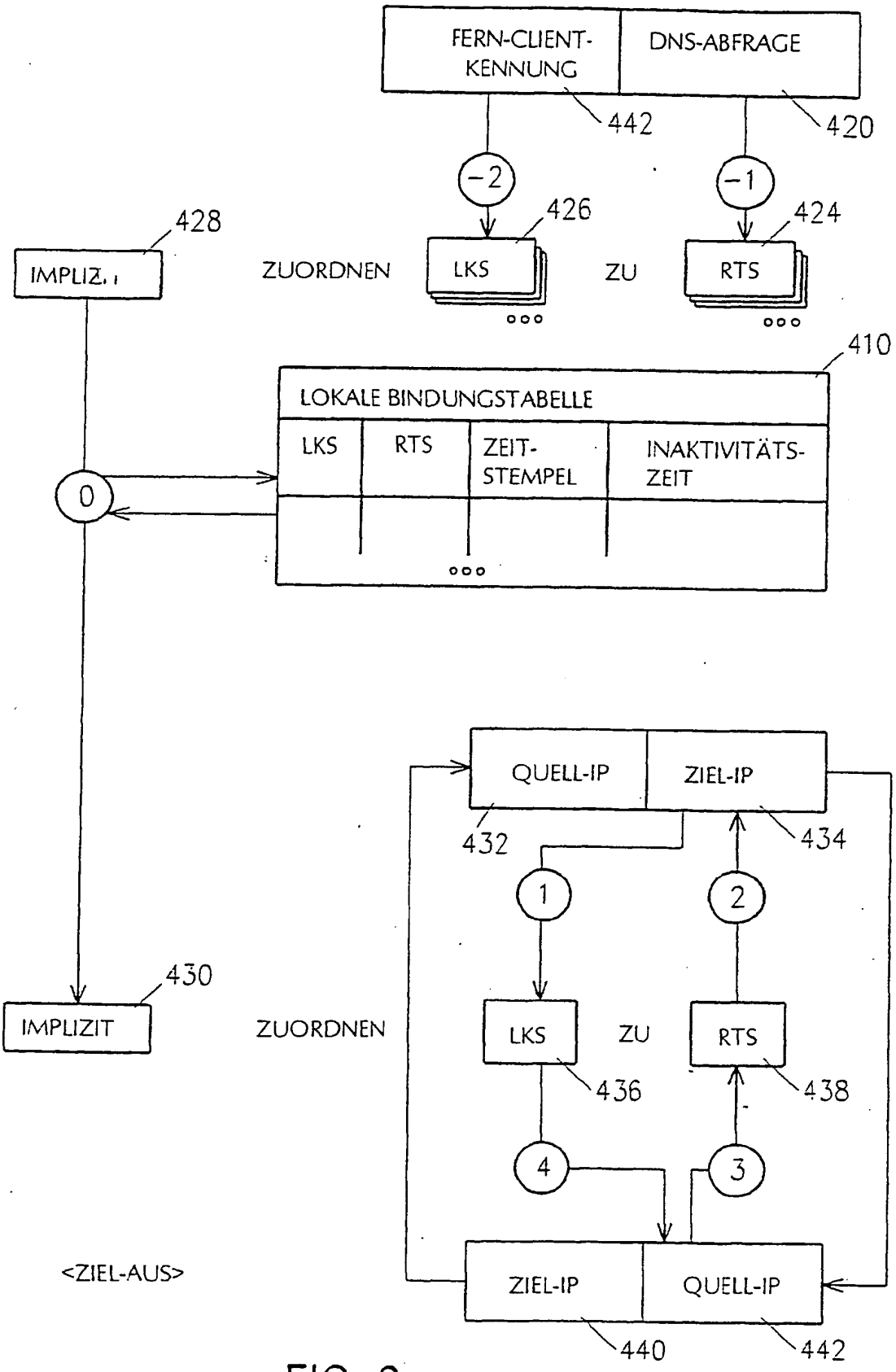
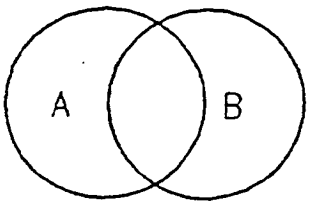


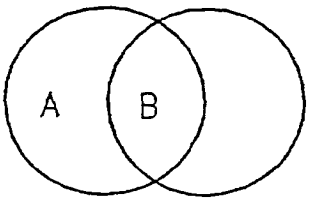
FIG. 6

Nummer: DE 101 28 493 A1
Int. Cl.[7]: H 04 L 12/46
Offenlegungstag: 3. Januar 2002

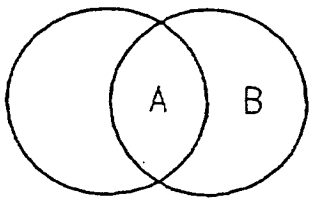
.ADRESSENDOMÄNEN



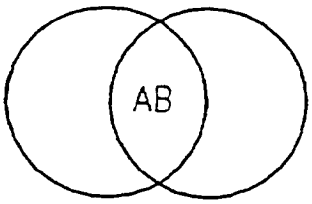
I. KEIN NAT



II. ERFORDERT NUR ZIEL-AUS-NAT



III. ERFORDERT NUR QUELLE-AUS-NAT



IV. ERFORDERT ZIEL-AUS-NAT UND QUELL-AUS-NAT

A ADRESSE VON HOST HINTER GATEWAY
B ADRESSE VON EXTERNEM HOST

FIG. 7

101 610/803